# STEGANOGRAFIJA U KONTEKSTU INFORMACIJSKE SIGURNOSTI

## STEGANOGRAPHY IN THE CONTEXT OF INFORMATION SECURITY

Džemal Kulašin
Nihad Čukle

**SAŽETAK**

U ovom radu predstavljaju se temeljna načela steganografije kao naučne (pod)discipline kriptografije bez koje je danas praktično neprovodiva zaštita informacionih sistema. U prvom redu, objašnjavaju se principi rada, te se potom steganografija dovodi u kontekst sa ključnim aspektima informacijske sigurnosti, označenih akronimom C-I-A (Confidentiality - Tajnost, Integrity - Cjelovitost i Accessibility - Dostupnost). Potom se u radu ukratko prikazuje korištenje jedne besplatne steganografske aplikacije, na primjeru sakrivanja povjerljivog podatka u grafičkoj datoteci.

*Ključne riječi: Steganografija, kriptografija, informacijska sigurnost*

**ABSTRACT**

This paper presents the basic principles of steganography as a scientific (sub)discipline of cryptography that is today indispensable in the protection of information systems. In the first place, the principles of work are explained, and then the steganography is brought into context with the key aspects of information security, marked with the Acronym C-I-A (Confidentiality, Integrity and Accessibility). Then, the paper briefly shows the use of a free steganographic application, for example, hiding confidential data in a graphical file.

*Keywords: Steganography, cryptography, Information security*

**UVOD**

Otvorenost informacionih sistema prema okolini u komunikacijskom smislu kroz Internet, uvjetuje da se informacijska sigurnost nameće kao jedan od ključnih faktora funkcioniranja poslovnih sistema. Stoga se informacijskoj sigurnosti danas posvećuje velika pažnja i traže novi načini podizanja sigurnosti na prihvatljivi nivo. U tim nastojanjima, u svijetu je sve prisutniji sistemski pristup, što je prepoznato i od strane međunarodne organizacije za standardizaciju (ISO) definiranjem standarda ISO 27001 koji daje podlogu za uspostavljanje tzv. ISMS-a, tj. Sistema upravljanja informacijskom sigurnosti (ISMS - Information Security Management System). Među obaveznim kategorijama Aneksa A, kao krucijalnog dijela ISO 27001, nalazi se i kriptografija. Razlog je jednostavan - kriptografijom se efikasno mogu (o)čuvati tajnost i integritet, kao dva glavna aspekta informacijske sigurnosti, te aspekt autentičnosti, što je posebno bitno u savremenoj digitalnoj komunikaciji. No, manje je poznato da je i steganografija dio kriptografije, te da se i steganografski alati itekako mogu koristiti u segmentu zaštite.

**POJAM STEGANOGRAFIJE**

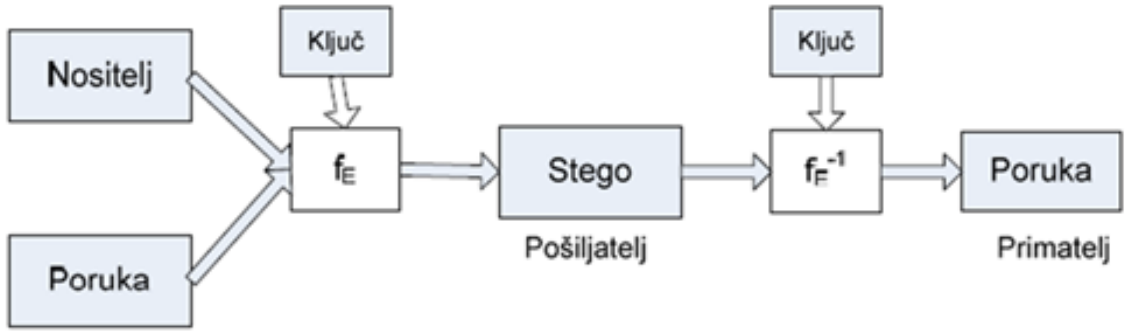
Steganografija se srstava u tzv. fizičku kriptografiju kojom se jedni podaci skrivaju u okviru nekih drugih podataka. Ova nekada jednostavna tehnika "skrivenog" pisanja (grč. steganos - skriveno, prikriveno, graphei - pisati), danas je uz digitalne tehnologije uznapredovala do oblasti koja ima značajnu

primjenu u očuvanju informacijske sigurnosti, posebno segmenata tajnosti i cjelovitosti. Upravo digitalna tehnologija daje pregršt mogućnosti za primjenu steganografije, uključujući i onu najrašireniju - metodu skrivanja informacija u digitalnoj slici. Stoga se moderna steganografija mahom i odnosi na skrivanje tajnih poruka u redundantnim dijelovima datotetaka (ovdje - datoteka nositelj). Naime, multimedijske datoteke u pravilu sadrže neupotrijebljene ili nevažne podatkovne prostore koje različite steganografske tehnike koriste tako da ih popune s tajnim informacijama. Takve datoteke se potom mogu razmjenjivati bez da iko bude svjestan prave svrhe dotične komunikacije. No, na žalost upravo zbog svog temeljnog principa nevidljivosti" informacija, steganografija se koristi i tokom ilegalnih aktivnosti, te je i njena problematika kompromitirajućeg konteksta.

## PRINCIP STEGANOGRAFIJE

Proces steganografije obično uključuje umetanje tajne poruke unutar nekog prenosnog medija koji se u tom slučaju naziva nositelj i ima ulogu prikrivanja postojanja tajne poruke. Nositelj mora biti takav skup podataka koji je sastavni dio uobičajene svakodnevne komunikacije te kao takav ne privlači posebnu pozornost na sebe, npr. tekst, slika, audio ili video zapis. Cjelina sačinjena od tajne poruke i nositelja unutar kojeg je ta poruka ugniježdena naziva se steganografski medij ili stego. Čak, u svrhu dodatne zaštite, moguća je i upotreba steganografskog ključa kojim se tajna poruka kriptira prije umetanja u nositelj [2].

*Slika 1: Steganografski sistem*




Oznake na Slici 1. imaju sljedeća značenja:

- fE: steganografska funkcija "ugrađivanje"
- fE-1: steganografska funkcija "izdvajanje"
- nositelj: medij unutar kojeg se sakriva tajna poruka
- poruka: tajna poruka koja treba biti sakrivena
- ključ: steganografski ključ; parametar funkcije fE
- stego: steganografski objekat

Od više tehnika steganografije, posebno je znakovita tzv. nulta šifra (eng. null cipher). Nulta šifra koristi se za sakrivanje informacija tako da se definira neki set pravila, npr. "čitaj svaku petu riječ" ili "čitaj svaki treći znak u svakoj riječi". Ova metoda omogućava skrivanje tajnih poruka u svakodnevnim porukama bez upotrebe kompliciranih algoritama ili alata.

Primjeri umetanja tajnog teksta unutar datoteka su, npr. ispod slike u PowerPoint datoteci, u Properties dijelu Word datoteke, unutar komentara na web stranicama, unutar bilo kojeg dokumenta tako da boja teksta odgovara boji pozadine, i sl. Jedan od

najjednostavnijih i najpoznatijih primjera primjene nulte šifre je poruka koju je jedan njemački špijun slao za vrijeme 2. svjetskog rata:

"APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS."

Uzimanjem svakog drugog slova iz svake riječi, dobiva se sljedeća tajna poruka:

"PERSHING SAILS FROM N.Y. JUNE 1" [5].

**LSB supstitucija**

LSB (eng. Least Significant Bit, Najmanje značajan bit) supstitucija jedna je od najčešćih steganografskih tehnika, gdje se najmanje značajni bitovi odabrane datoteke nositelja zamijene se bitovima tajne poruke. Ova tehnika se posebno jednostavno primjenjuje na slikovne datoteke. Naime, ovdje se velika količina informacija može sakriti malim ili potpuno neuočljivim utjecajem na datoteku nositelja skrivene informacije. Na primjer, želimo li sakriti tekstualnu poruku u svaki bajt 24-bitne slike, možemo spremiti 3 bita u svaki piksel (1 bit u kanal svake boje). Slika dimenzija 1024x768 piksela može sakriti 1024 * 768 * 3 = 2359296 bitova informacija. To je 294912 bajta ili 288 kilobajta informacija. To je velika količina, no stego slika ljudskom oku izgleda (gotovo) identično kao i original.

Pretpostavimo da želimo "sakriti" tekstualnu poruku - slovo A. Njegov ASCII ekvivalent iznosi 65(10), što je binarno 01000001(2). Za skrivanje su nam dovoljna 3 piksela. Npr. neka su ti pikseli sljedeći:

(00100111, 11101001, 11001000)
(00100111, 11001000, 11101001)
(11001000, 00100111, 11101001).

Umetanje binarne vrijednosti slova A u tri piksela rezultira novom binarnom situacijom:

(00100110, 11101001, 11001000)
(00100110, 11001000, 11101000[1])
(11001000, 00100111, 11101001).

U prosjeku se primjenom ove metode promijeni samo polovica najmanje značajnih bitova. Piksel koji se najviše promijenio, promijenio se za dvije nijanse, što je u odnosu na 16,7 miliona nijansi zanemarivo za ljudsko oko [7].

Dakle, ako želimo sakriti tajnu poruku unutar slikovne datoteke, prvi korak je odabir datoteke nositelja. Nakon što su datoteka-nositelj i tajna poruka odabrane, bira se podskup najmanje značajnih bitova datoteke-nositelja. Broj bitova u odabranom skupu odgovara broju bitova tajne poruke. Tada se nekim redoslijedom svaki prikrivni bit zamjenjuje bitom tajne poruke, sve dok svi nisu zamijenjeni. U najjednostavnijem slučaju LSB supstitucije tajni se bitovi pohranjuju u najmanje značajni bit (LSB) svakog piksela po redu.

**IMAGE DOWNGRADING**

Image downgrading tehnika podrazumijeva sakrivanje cijele slikovne datoteku u drugu slikovnu datoteku, upravo manipuliranjem najmanje značajnih bitova. Razlike u izgledu datoteka, pogotovo na kraju procesa zamjene najmanje/najviše značajnih bitova prilično budu malene, te ih (inače) nesavršeno ljudsko oko često i ne može primijetiti.

Pretpostavimo da pošiljalac želi tajno prenijeti slikovnu datoteku aviona F15, što u ovom slučaju predstavlja tajnu datoteku (Slika 2).

1 Samo su boldirani bitovi (3 bita od 9 najmanje značajnih) koji su promijenili vrijednost!

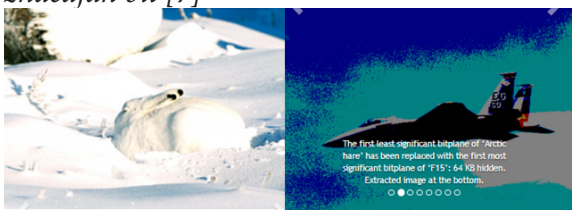
*Slika 2: Tajna datoteka - F15 [8]*

U tom slučaju treba odabrati i drugu (uglavnom bezazlenu) sliku istih dimenzija, koja će mu poslužiti kao datoteka nositelj. Npr. to može biti (naivna) slikovna datoteka zimskog zeca, predstavljeno na Slici 3.

*Slika 3: Datoteka nositelj - Zimski zec [8]*

Kada se odaberu dvije slike istih dimenzija, zamjenjuju se 4 najmanje značajna bita u prikazu boje svakog piksela datoteke nositelja sa 4 najviše značajna bita prikaza boje piksela tajne slike koji se nalaze na istom mjestu, čime se dobija tzv. stego datoteku. Primatelj izvlači četiri najmanje značajna bita svakog elementa stego datoteke i tako dobiva najviše značajne bitove tajne datoteke. Kada dobije po 4 najznačajnija bita svake vrijednosti boje u svakom pikselu, ta četiri nadopuni sa još četiri bita, npr. s nulama, i dobija se aproksimacija tajne slike koja izgleda dijelom narušena, ali ipak iskoristiva (tajna) datoteka (Slika 4) [7].

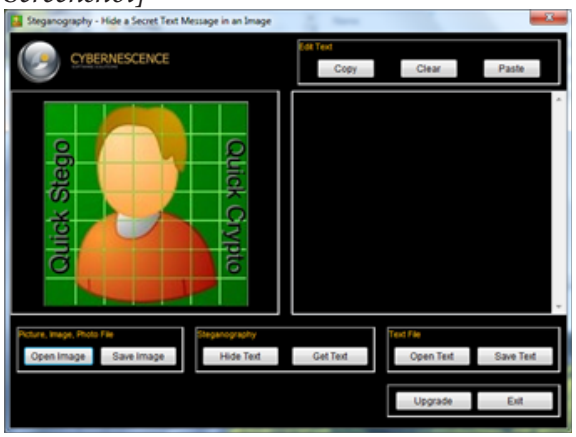
*Slika 4: Aproksimacija: prvi najmanje/najviše značajan bit [7]*




## PRIMJER STEGANOGRAFSKE APLIKACIJE

Postoji veliki broj steganografskih aplikacija, koje se mogu i potpuno besplatno koristiti; jedna od takvih aplikacija je i Quick Stego[2] (Slika 5). U ovom dijelu pokazat ćemo koliko je trivijalan posao sakriti određene podatke koristeći gotova programska rješenja, poput alata Quick Stego.

*Slika 5: Steganografski alat Quick Stego [Izvor: Screenshot]*




Npr. pretpostavimo da unutar grafičke datoteke Desert.jpeg važan, odnosno povjerljiv podatak rikJlDjf78?A. Nakon što pokrenemo aplikaciju, biramo opciju za uvom grafičke datoteke, te u radnom prostoru aplikacije upisujemo povjerljivi podatak (Slika 5).

2 http://quickcrypto.com/free-steganography-software.html

Preostali dio posla je odabrati opciju Hide Text. Time je povjerljivi podatak sakriven unutar grafičke datoteke, što naravno nije vidljivo vizuelnim pregledom. Da bi se pronašli sakriveni podaci, potrebno je provesti tzv stegoanalizu, koja može biti otežana eventualnom enkripcijom.

## DIGITALNI VODENI ŽIG

Digitalni vodeni žigovi (eng. watermark) su (relativno) novo područje u steganografiji, odnosno digitalnoj obradi signala i komunikacijama. Svrha vodenog žiga je omogućavanje zaštite multimedijskih dokumenata u smislu autorskog prava, zaštite kopiranja (eng. copyright protection), kojeg već postojeće tehnologije ne rješavaju. Ideja takve zaštite je skrivanje podataka vodenog žiga u originalnom dokumentu, bilo da je riječ o fotografiji, kao najčešćem formatu, ili drugom multimedijskom formatu (audio formati, video formati, 3D modeli, računarski programi i sl.). Osnovna podjela digitalnog vodenog žiga je na tzv. vidljivi vodeni žig (eng. visible digital watermark) i tzv. nevidljivi vodeni žig (eng. invisible digital watermark).

Vidljivi vodeni žigovi danas imaju puno manju primjenu od nevidljivih žigova, a najčešće se koriste na dokumentima u obliku loga. Svrha je da naznači zaštićenost sadržaja i da onemogući njegovo korištenje bez dozvole autora. Vidljivi vodeni žig se dodaje jednostavnom metodom na originalnu sliku dok je reverzibilan postupak moguć uz poznavanje tačnog formata žiga ili uz trud i vještinu pomoću nekog programa za složeniju obradu slike. Za razliku od vidljivih vodenih žigova, nevidljivi su sakriveni unutar sadržaja slike, neprimjetni ljudskom oku te ih je moguće detektirati isključivo softverom specijalne namjene [3].

Iz osnovne podjele prema vizuelnoj percepciji, u kombinaciji sa robusnošću digitalnog vodenog žiga, proizilazi i dvojna podjela na tzv. robustan nevidljiv vodeni žig i tzv. lomljiv nevidljiv vodeni žig. Robustan nevidljiv vodeni žig (eng. Invisible – Robust watermark) je vizuelno nevidljiv, ali ga detektira dekoder. Ovaj žig karakterizira otpornost na napade (npr. JPEG kompresija ne može uništiti žig). Kod lomljivog nevidljivog žiga (eng. Invisible – Fragile watermark) žig je također nevidljiv, ali se može detektirati. Ovaj žig karakterizira neotpornost na sve vrste napada (npr. ne prolazi JPEG kompresiju) [1].

### Implementacija vodenog žiga

Za implementaciju digitalnog vodenog žiga postoje brojne metode koje se dijele s obzirom na domenu u kojoj se radi. Tako, žigovi se mogu unositi u prostornoj domeni (eng. spatial domain), frekvencijskoj domeni (eng. frequency domain ) te wavelet domeni (eng. wavelet domain). Najčešće metode implementacije vodenog žiga su LSB metoda, Korelacija i CDMA metoda te DCT metoda. [4]

Najjednostavnija metoda postavljanja vodenog žiga unutar neke slike je LSB metodom, tj. kada žig postavljamo na bitove slike koji su od najmanjeg značaja. Tako se dobija visoko kapacitetni kanal kojim se mogu ‘’unijeti” manji objekti u sliku više puta. Kada bi se slika podvrgnula različitim modifikacijama (kompresija, dodavanje šuma ili distorzije) većina objekata bi bila izgubljena, samo jedan preživjeli vodeni žig bi se smatrao uspjehom. LSB supstitucija međutim uprkos svojoj jednostavnosti ima i brojne nedostatke. Iako bi vodeni žig mogao preživjeti transformacije kao što su obrezivanje, dodavanje šuma ili sažimanje uz gubitak, mogao bi se i izgubiti. Najbolji napad na vodeni žig a da slika u koju je unesen ostane nepromijenjena, bio bi da se jednostavno postave svi LSB bitovi na jedinicu. Poboljšanje u odnosu na osnovnu LSB supstituciju, bilo bi korištenje generatora pseudo-slučajnih brojeva kako bi se utvrdilo koji će se pikseli koristiti za ugrađivanje

žiga, na temelju ključa. LSB modifikacija dokazuje da je prilično jednostavan i moćan alat za stenografiju, međutim, nedostaje mu osnovna robusnost koju zahtijevaju aplikacije za postavljanje vodenih žigova.
Metoda korelacije pokazuje bolje rezultate od LSB, pogotovo kad je u pitanju šum, zamućenje i sl. Međutim, ta poboljšanja imaju za posljedicu jako lošu kvalitetu slike gdje je oku vidljiva podjela slike na blokove. Bolja verzija ove metode je CDMA metoda (eng. Code Division Multiple Access) gdje je šum jednoliko raspoređen po cijeloj slici, a ne po blokovima. Uz to, CDMA daje još bolje rezultate pri uticaju šuma i zamućenja od metode korelacije, ali ponovno kao posljedicu ima još manji kvalitet slike izraženu objektivnom mjerom PSNR (engl. Peak signal-to-noise ratio - odnos najviše vrijednosti signala i nivoa šuma).
DCT metoda (eng. Discrete Cosine Transform) pokazuje visoku otpornost JPEG kompresije kao i značajnu količinu zamućenja i šuma. Inače, ova metoda vrlo je popularna u svijetu digitalne tehnologije upravo zbog otpornosti na JPEG kompresiju, ali i što se unosi vrlo mala disperzija u sliku te zbog mogućnosti detektiranja watermark-a direktno u transformiranoj domeni, što utiče na brzinu detekcije [4].

## ZAKLJUČAK

Steganografija je (manje poznata) metoda kriptografije kojom se jedni podaci prikrivaju u okviru nekih drugih podataka. Ova nekada jednostavna tehnika "skrivenog, prikrivenog pisanja" uznapredovala je do oblasti koja danas ima značajnu primjenu u očuvanju informacijske sigurnosti, posebno segmenata tajnosti i cjelovitosti. Naravno, načela steganografije su drugačija jer se ne vrši enkripcija podataka kao u kriptografiji, već se zaštita postiže sakrivanjem povjerljivih podataka unutar drugih podataka, tj. datoteka.
No, treba naglasiti da je (i) steganografija kontroverzna disciplina, jer je zbog svojih mogućnosti interesno područje različitih involviranih strana, često dijametralno suprotnih načela i pristupa. Problematika je eskalirala dostupnošću jeftinih, ali moćnih računarskih sistema, koji u rukama pojedinaca postaju izuzetno moćan steganografski alat.

## LITERATURA

[1] CARNET, Digitalni vodeni žigovi, (2010), [dostupno na: http://www.cert.hr/sites/default/files/ NCERT-PUBDOC-2010-08-310.pdf]
[2] CARNET, Steganografija (2011), dostupno na: [http://www.cert.hr/sites/.../CCERT-PUBDOC-2006-04-154.p]
[3] Hausknecht, K. i dr. (2010): Skrivanje podataka u slici, dokumentacija, Fakultet elektrotehnike i računarstva Zagreb [dostupno na: https://www.fer.unizg.hr/_download/repository/Skrivanje _ Podataka_u_Slici_Dokumentacija.pdf]
[4] Dujella, A. Kriptografija, (2007), [dostupno na: https://web.math.pmf.unizg.hr/~duje/ kript/kriptografija.html]
[5] Johnson, N., Duric, Z., Jajodia, S. (2001): Information hiding - Steganography and Watermarking atacks and countermeasures, Springer Science Business Media, LLC (2011):
[6] Kriptografija kroz primjere, Udžbenici Univerziteta u Bihaću, Pedagoški fakultet Bihać, Bihać.
[7] Škorić, N. (2005), Kriptografija kroz primjere, Fakultet elektrotehnike i računarstva, Zagreb, [dostupno na: http://os2.zemris.fer.hr/algoritmi/simetricni/2005_skoric/seminar/index.html]
[8] Zeljković, S. (2009), Steganografija, Math.e - elektronski matematički časopis, broj 5. [dostupno na: http://e.math.hr/stegano/index.html]